

## REMARKS

The Examiner is thanked for the performance of a thorough search.

Claims 1-3, 11-14, 24, and 26-28 have been amended. Claims 1-28 are pending in the application.

### REJECTIONS NOT BASED ON THE CITED ART

Claims 1-11 and 26-28 were rejected under 35 USC 112, second paragraph, for allegedly lacking antecedent basis for the term “the shared secret value.” The amendments to the claims herein remedy the problem noted in the Office Action. For example, Claims 1 and 26-28 now recite a “second” shared secret key value to distinguish that shared secret key value from the “initial” shared secret key recited in those claims. Therefore, withdrawal of the rejections of Claims 1-11 and 26-28 under 35 USC 112, second paragraph, is respectfully requested.

### REJECTIONS BASED ON THE CITED ART

Claims 1-5, 7-15, 17-20, and 22-28 were rejected under 35 U.S.C. §102(b) as being anticipated, allegedly, by U.S. Patent No. 5,668,877 to Aziz (“Aziz”).

Claims 6, 16, and 21 were rejected under 35 U.S.C. §103(a) as being unpatentable, allegedly, over Aziz in view of U.S. Patent No. 6,295,361 to Kadansky, et al. (“Kadansky”).

The rejections are traversed for the reasons discussed below.

#### *Claims 1-5, 7-10, and 26-28*

Claim 1 recites the features “receiving a **third public key value** from a third node that seeks to join the first network communication entity;” and “**creating a second shared secret key value based on** the collective public key value and the **third public key value.**”

Thus, unless Aziz discloses a second shared secret key that is **created based on** both (a) a collective public key value and (b) a third public key value received from a third node that seeks to join a network communication entity, Aziz does not anticipate Claim 1 under 35 U.S.C. §102(b).

Beginning in column 14, Aziz discloses that a group interchange key  $K_g$  may be used as a key-encrypting key for communication in a multicast group. Nodes in a multicast group use  $K_g$  to encrypt a randomly-generated packet encryption key  $K_p$ . The nodes use  $K_p$  to encrypt content that the nodes need to protect from those outside the group. The nodes send the encrypted content and the encrypted key  $K_p$  (but not  $K_g$ ) to the multicast address. Nodes that subscribe to the multicast address use  $K_g$  to decrypt  $K_p$ . Once these nodes have decrypted  $K_p$ , these nodes can decrypt the content using  $K_p$ . A different  $K_p$  may be sent with each transmission.

However, in order for this secret group communication to be achieved, each node in the multicast group first needs to obtain  $K_g$ . Aziz discloses that a group owner sends  $K_g$  to a requesting node in an encrypted packet using the **pairwise secure protocol** described earlier in Aziz's specification (col. 14, lines 23-32). This pairwise protocol is described beginning in column 3. A node I and a node J exchange public values, so that node I obtains node J's public value, and node J obtains node I's public value. Node I and node J also each have private values that they do not exchange with each other. Using node I's private value and node J's public value, node I derives a key  $K_{ij}$ . Using node J's private value and node I's public value, node J also derives key  $K_{ij}$ .

Once node I and node J both have derived  $K_{ij}$ , node I can send data secretly to node J by encrypting that data using  $K_{ij}$ . For example, suppose that node J is the requesting node that wants to engage in secret group communication with a multicast group that includes node I. Node J needs  $K_g$  to do so. According to Aziz, in order for node J to obtain  $K_g$ , node I and node J

first engage in the pairwise secure protocol to derive  $K_{ij}$ . Then, node I encrypts  $K_g$  using  $K_{ij}$ , and sends the encrypted  $K_g$  to node J. Node J decrypts  $K_g$  using  $K_{ij}$ . Thereafter, nodes I and J can use  $K_g$  to communicate secretly with each other and any other member of the group that also knows  $K_g$ .

The Office Action appears to analogize the “second shared secret key value” to  $K_g$ . However, although  $K_{ij}$  is used to encrypt  $K_g$  for transmission to a prospective group member that does not yet have  $K_g$ ,  $K_g$  is not created from or based in any way on  $K_{ij}$ . In Aziz, when a group owner sends  $K_g$  to a requesting node, the group owner does **not** in any way **create**  $K_g$  based on any public key value of the requesting node. Regardless of the number of nodes that request  $K_g$  from the group owner, the value of  $K_g$  never differs. A first requesting node will get  $K_g$  from the group owner. A second requesting node will get the same  $K_g$  from the group owner. A hundredth node will get the same  $K_g$  from the group owner. Presumably, the public key values of these requesting nodes would necessarily differ from each other.  $K_g$  has nothing to do with any public key values of any of these nodes.

Because  $K_g$  is not created based on any public key value of any requesting node,  $K_g$  is **not** analogous to the second shared secret key value recited in Claim 1.

As discussed above, in Aziz,  $K_g$  is used to encrypt a randomly-generated packet encryption key  $K_p$ .  $K_p$  is randomly generated (col. 15, lines 32-34). Like  $K_g$ ,  $K_p$  is not created based on any public key value of any requesting node. Thus,  $K_p$  is also **not** analogous to the second shared secret key value recited in Claim 1.

Neither  $K_g$  nor  $K_p$  is a “second shared secret key” that is created based on a third public key value of a third node that seeks to join a first network communication entity as required by Claim 1. There does not appear to be any shared secret key disclosed in Aziz that possesses the recited characteristics of the “second shared secret key” of Claim 1.

Additionally, the “second shared secret key” of Claim 1 must be created based **also** on a “collective public key value” that is generated based on both (a) a “first private key value” and (b) a “second private key value” that is derived from a “second public key value” that is received from a “second node.” There does not appear to be any shared secret key disclosed in Aziz that is created based on a “collective public key value” having these qualities.

Thus, Claim 1 recites features that Aziz does not disclose. Consequently, Claim 1 is patentable over Aziz under 35 U.S.C. §102(b).

If the next Office Action maintains this rejection, Applicants respectfully request that the next Office Action expressly state what elements, in Aziz, are supposed to correspond to (a) the “second shared secret key value,” (b) the “third public key value,” and (c) the “collective public key value” of Claim 1, and what portion of Aziz discloses that the element supposedly analogous to the “second shared secret value” is created based on the elements supposedly analogous to the “third public key value” and the “collective public key value.”

Claims 2-5, 7-10, and 28 comprise the distinguished features of Claim 1 by virtue of their dependence from Claim 1. Therefore, Claims 2-10 and 28 are likewise patentable over Aziz under 35 U.S.C. §102(b).

Claim 26 recites a computer-readable medium carrying instructions which, when executed, cause the steps of the method of Claim 1 to be performed. Claim 27 recites a server that comprises means for performing the steps of the method of Claim 1. Therefore, for at least the reasons discussed above with regard to Claim 1, Claims 26 and 27 are patentable over Aziz under 35 U.S.C. §102(b).

*Claims 11-15 and 17-19*

Claim 11 recites “creating the group shared secret key based on the collective public key value and the private key value associated with the first node;” where the “collective public key value is shared by each other node in the first network communication entity” and the “first node” is “joining the first network communication entity.”

Oddly, the Office Action cites no specific sections of Aziz in its rejection of Claim 11.

The “group shared secret key” of Claim 11 is similar to the “second shared secret key” of Claim 1. In order for a secret key to be analogous to the “group shared secret key” of Claim 11, that secret key must be **created based on** both (a) a collective public key value of the group and (b) a private key value of the node that is joining the group.

As is discussed above with regard to Claim 1, neither  $K_g$  nor  $K_p$  of Aziz possesses these characteristics. Aziz does not appear to disclose any group shared secret key that is created based on both (a) a collective public key value of the group and (b) a private key value of the node that is joining the group.

Thus, Claim 11 recites features that Aziz does not disclose. Consequently, Claim 11 is patentable over Aziz under 35 U.S.C. §102(b).

Claims 12-15 and 17-19 comprise the distinguished features of Claim 11 by virtue of their dependence from Claim 11. Therefore, Claims 12-15 and 17-19 are likewise patentable over Aziz under 35 U.S.C. §102(b).

*Claims 20 and 22-25*

Claim 20 recites “**computing** a new shared secret key by the new node **based upon** the common public key of the multicast group and the new private value;” where the “new private value” is generated by a “new node” that joins the multicast group. Thus, the “new shared secret

key” of Claim 20 must be computed based upon both (a) “the common public key of the multicast group” and (b) a new private value generated by a new node that joins the multicast group.

Oddly, the Office Action cites no specific sections of Aziz in its rejection of Claim 20.

As is discussed above with regard to Claims 1 and 11, Aziz does not disclose any shared secret key that is computed based specifically upon such keys and values. Consequently, Claim 20 is patentable over Aziz under 35 U.S.C. §102(b).

Claims 22-25 comprise the distinguished features of Claim 20 by virtue of their dependence from Claim 1. Therefore, Claims 22-25 are likewise patentable over Aziz under 35 U.S.C. §102(b).

#### *Claims 6, 16, and 21*

Claims 6, 16, and 21 depend from various claims discussed above. By virtue of this dependence, Claims 6, 16, and 21 comprise the features of the claims from which they depend—features that were distinguished from Aziz above.

The Office Action does not rely on Kadansky to disclose these distinguished features. The Office Action only relies on Kadansky to disclose, allegedly, the step of storing and distributing public values using a key distribution center. Since neither Aziz nor Kadansky discloses the distinguished features discussed above, even the combination of Kadansky with Aziz lacks the distinguished features of Claims 6, 16, and 21.

Therefore, Claims 6, 16, and 21 are patentable over the combination of Aziz and Kadansky under 35 U.S.C. §103(a).

## CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

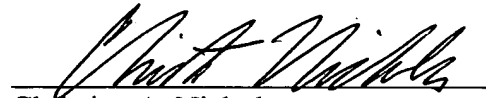
The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to deduct any applicable fees from and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: September 27, 2005



Christian A. Nicholes  
Reg. No. 50,266

2055 Gateway Place, Suite 550  
San Jose, California 95110-1089  
Telephone No.: (408) 414-1080 ext. 224  
Facsimile No.: (408) 414-1076